

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
нормативного освітнього компонента
ПІДГОТОВКА ДО ЄДКІ
Підготовки першого (бакалаврського) рівня вищої освіти
Спеціальності 125 Кібербезпека та захист інформації
Освітньо-професійної програми Кібербезпека та захист інформації

Луцьк – 2024

Силабус нормативного освітнього компонента Підготовка до ЄДКІ підготовки бакалаврів, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації

Розробники:

Чернящук Наталія Леонідівна, доктор педагогічних наук, професор, професор кафедри комп'ютерних наук та кібербезпеки

Погоджено

Гарант освітньо-професійної програми:



Чернящук Н.Л.

Силабус освітнього компонента затверджено
комп'ютерних наук та кібербезпеки

на засіданні кафедри

протокол № 4 від 21.11.2024 р.

Завідувач

кафедри:



Гришанович Т. О.

I. Опис ОК

Найменування показників	Галузь знань, спеціальність, освітньо- професійна програма, освітній рівень	Характеристика навчальної дисципліни
		Нормативна
Денна форма навчання	Галузь знань 12 Інформаційні технології, спеціальність 125 Кібербезпека та захист інформації, освітньо-професійна програма Кібербезпека та захист інформації освітній рівень бакалавр	Рік підготовки 4
Кількість Годин/кредитів 60/2		Семестр 8
		Самостійна робота 56 год.
		Консультації 4 год.
		Форма контролю: без форми контролю, як допуск до ЄДКІ
Мова навчання – Українська		

II Інформація про викладача

ППП: Черняшук Наталія Леонідівна;

Науковий ступінь: доктор педагогічних наук;

Вчене звання: професор;

Посада: професор кафедри комп'ютерних наук та кібербезпеки;

Контактна інформація: Cherniashchuk.Nataliia@vnu.edu.ua

Дні занять: <http://94.130.69.82/cgi-bin/timetable.cgi>

III. Опис дисципліни

Анотація курсу. Перший (бакалаврський) рівень вищої освіти відповідає сьомому рівню Національної рамки кваліфікацій і передбачає здобуття особою теоретичних знань та практичних умінь і навичок, достатніх для успішного виконання професійних обов'язків за обраною спеціальністю. На цьому рівні здобувається ступінь бакалавра.

Бакалавр – освітній ступінь, що здобувається на першому рівні вищої освіти та присуджується закладом вищої освіти у результаті успішного виконання здобувачем вищої освіти освітньо-професійної програми, обсяг якої становить 180-240 кредитів ЄКТС. <http://surl.li/zbucrd>

ЄДКІ – це іспит на кшталт ЗНО/НМТ для випускників бакалаврату, зокрема спеціальності 125 Кібербезпека та захист інформації, у формі комп'ютерного тестування, який проходить під наглядом незалежних представників та відеоспостереженням у спеціально облаштованих аудиторіях. ЄДКІ проводять відповідно до Наказу Міністерства освіти і науки України Про затвердження Програми єдиного державного кваліфікаційного іспиту зі спеціальності Кібербезпека на першому (бакалаврському) рівні вищої освіти №980 від 04.11.2022.

Пререквізити: освітні компоненти передбачені ОПП (ОК1-ОК36).

Постреквізити: ЄДКІ.

Мета – оцінювання рівня фахових та предметних компетентностей, необхідних для ефективного виконання професійної діяльності за обраною спеціальністю.

Результати навчання:

Інтегральна компетентність: здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки.

Загальні компетентності:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК 4. Здатність спілкуватися іноземною мовою.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.

ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні компетентності:

СК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК 4. Здатність забезпечувати захист інформації інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)

СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання:

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН 3. Застосовувати принципи неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати

оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН 7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН 8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН 15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

РН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

РН 20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Структура ОК і політика оцінювання: <http://surl.li/zbucrd>

Підготовка до ЄДКІ здійснюється у відповідності до програми <http://surl.li/zbucrd> у разі зміни програми, інформацію буде подано додатково.

Рекомендована література та інтернет-ресурси:

1. ДСТУ ISO/IEC 27002: 2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27003: 2013, IDT).
2. ДСТУ ISO/IEC 27005: 2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005: 2018, IDT).
3. Закон України "Про захист інформаційно- телекомунікаційних системах". <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
4. Закон України "Про інформацію". <https://zakon.rada.gov.ua/laws/main/2657-12>
5. Закон України "Про основні засади забезпечення кібербезпеки України" <https://zakon.rada.gov.ua/laws/main/2163-19>
6. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 с. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 с.
7. Лаптев О.А., Кузавков В.В., Хорошко В.О. «Системи пошуку засобів негласного здобуття акустичної інформації» – К. Міленіум. 2023 – 282 с. https://www.researchgate.net/publication/368925556_SISTEMI_POSUKU_ZASOBIV_NEGLASNOGO_ZDOBUTTA_AKUSTICNOI_INFORMACII
8. Указ Президента України №446/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"
9. A.O. Korchenko, V.O. Breslavskyi, S.P. Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2021.225346.
10. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615.
11. Управління інформаційною безпекою: Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузі знань 12 Інформаційні технології спеціальності 125 «Кібербезпека» денної та заочної форм навчання» / укладач Н.Л. Черняшук, Луцьк: ЛНТУ, 2022. 120 с.
12. Управління інформаційною безпекою: Методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузі знань 12 Інформаційні технології спеціальності 125 «Кібербезпека» денної та заочної форм навчання» / укладач Н.Л. Черняшук. Луцьк: ЛНТУ, 2022. 34 с.
13. Управління інформаційною безпекою: Методичні вказівки до самостійної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» галузі знань 12 Інформаційні технології спеціальності 125 «Кібербезпека» денної та заочної форм навчання» / укладач Н.Л. Черняшук. Луцьк: ЛНТУ, 2022. 24 с.

14. Serhii Yevseiev, Volodymyr Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 c.
15. A.O. Korchenko, V.O. Breslavskiyi, S.P. Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2021.225346.
16. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615.
17. Євсєєв С.П. , Король О.Г. , Шматко О.В. Кібербезпека: криптографія з PYTHON]. —Новий світ-2000, 2024. — 120с
18. Головін М.Б., Головіна Н.А., Яцюк С.М., Сачук Ю.В. Захист інформації стегаграфічним способом мовою Python засобами графічної бібліотеки Pillow. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк, 2020. Випуск № 40 с.110-115. URI: <https://evnuir.vnu.edu.ua/handle/123456789/19701>
19. Головін М.Б., Головіна Н.А. Навчальний приклад маскуванню інформації в акустичному сигналі. Наукові записки Бердянського державного педагогічного університету. Серія: Педагогічні науки. Бердянськ, 2021. Випуск 2. С. 203-210. URI: <https://evnuir.vnu.edu.ua/handle/123456789/20108>
20. Mykola Holovin, Nina Holovina Educational example of masking textual information in a photographic signal. Journal «ScienceRise: Pedagogical Education» No4(49)2022 pp24-28 URL: http://journals.urau.ua/sr_edu/article/view/261051/258566
21. Головін М.Б., Головіна Н.А. Фур'є перетворення в якості аплікації спектрального аналізу звуків у курсах комп'ютерної фізики та захисту інформації. Комп'ютерно- інтегровані технології: освіта, наука, виробництво. Луцьк, 2021. Випуск № 42. С.37-42. URI: <https://evnuir.vnu.edu.ua/handle/123456789/19750>
22. Документація Python 3.8.12. URL: <https://docs.python.org/3.8/index.html>
23. Serhii Yevseiev, Volodymyr Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 c. Serhii Yevseiev, Volodymyr Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 c.
24. Лаптев О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. К. ДУТ. 2020 – 126 с. <https://dut.edu.ua/ua/lib/2/category/96/view/2031>
25. О.А. Лаптев. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. Міленіум. 2020 – 326 с. УДК 004.056.53. ISBN 987-966-8063-79-3. https://www.dut.edu.ua/uploads/1_2162_16683938.pdf
26. Лаптев О.А., Кузавков В.В., Хорошко В.О. «Системи пошуку засобів негласного здобуття акустичної інформації» – К. Міленіум. 2023 – 282 с. https://www.researchgate.net/publication/368925556_SISTEMI_POSUKU_ZASOBIV_NEGLASNOGO_ZDOBUTTA_AKUSTICNOI_INFORMACII
27. Указ Президента України №446/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"
28. A.O. Korchenko, V.O. Breslavskiyi, S.P. Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109),

2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2021.225346.

29. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615.